UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/989,479	11/20/2001	Todd D. Graham	1048-024	1151

80360   7590   11/07/2008
Bainwood, Huang & Associates, LLC
2 Connector Road
Westborough, MA 01581

EXAMINER
CHANKONG, DOHM

ART UNIT	PAPER NUMBER
2452	

MAIL DATE	DELIVERY MODE
11/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 September 2008_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-19_ is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-19_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to Applicant's arguments filed on 9/16/2008. Claims 17-19 are

added. Claims 1-19 are presented for further examination.

2.   This is a final rejection.

Response to Arguments

3.   Applicant argues that none of the cited prior art references disclose (1) a client device

with one or more communication means via which said content and said usage rights are

provided to said client device or (2) a proxy system comprising an access control module

configured to selectively obtain content comprising data blocks on an individual block basis. As

to the former argument, Applicant argues that Rabne merely discloses providing right manage

compliant (RMc) browsers to a client but does not disclose sending usage rights. However,

Applicant's argument ignores Rabne's teaching that the RMc browsers "enforce the functionality

that is available to a user," for example, by "'gray[ing] out in a Windows environment things

such as capability to print, download, etc. if a user does not have those sort of rights or

permissions." Because the RMc browsers are located at the client and because the RMc

browsers enforce the user permissions for the content, Rabne clearly implies that the user

permissions are sent to the client device (via the RMc browsers). In the above example, user

access rights such as whether the user has the capability to print must be sent to the client in

order inform the RMc browser as to which "thing" to gray out [see Rabne, column 8 «lines 16-

19»: returning the permissions to the user].

As Applicant's latter argument, Applicant argues that "a 'block' is a unit of data storage. while a 'packet' is a unit of data transmittal." Applicant's specification discloses a file that is divided into a plurality of data blocks and each block is transmitted between a client and server [Applicant's patent publication 200200178271, 0235 & 0271]. Moreover, in Applicant's claims, the content sources are transmitting data blocks to the proxy system. Clearly, as indicated by both Applicant's claims and specification, the claimed "blocks" are being used as a means of transmitting data over a network. "Packets" are well known in the art as a "a block of information that is transmitted within a single transfer operation" ["The Authoritative Dictionary of IEEE Standard Terms", Seventh Edition, pg. 789]. Based on the foregoing, Taylor's packets read on the claimed "block."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabne et al. (U.S. Patent Number 6,006,332), hereinafter referred to as Rabne, in view of O'Brien et al, U.S. Patent No. 6.658.571 ["O'Brien"], further in view of Taylor et al, U.S Patent No. 6.728.885 ["Taylor"].

5.   Rabne disclosed a system for controlling access to and protecting use of digitized data

utilizing a secure rights management server. In an analogous art, O'Brien is directed towards a

security framework utilizing kernel-based security modules to protect file systems by controlling

access to and protecting use of computer files. Also in an analogous art, Taylor disclosed a

security system for filtering packets by utilizing, in part, a module operating at the kernel level to

examine packets to protect computer systems.

6.   Concerning claims 1 and 9, Rabne did not explicitly state a client module configured to

interface to a client operating system kernel and configured to enforce a set of usage rights

within the operating system kernel without application rewrites, wherein enforcing the set of

usage rights includes: intercepting a system call between an application and the client OS,

evaluating the system call based on the set of usage rights, and blocking or modifying the system

call based on said evaluation. However, allowing a system to enforce access rights in an

operating system kernel by intercepting system calls and evaluating the system call based on the

access rights was a well known feature in the art as evidenced by O'Brien whose system uses a

security mechanism at the operating system level to determine usage rights for users or

processes. Further, as discussed above, the limitation "without application rewrites" is merely an

effect of performing the enforcement within the OS kernel. Thus, since O'Brien discloses

enforcing usage rights at the OS level, O'Brien implicitly teaches the limitation. It would have

been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify

the system of Rabne by adding the ability to use a client module configured to interface to a

client operating system kernel and configured to enforce a set of usage rights within the

operating system kernel by intercepting system calls and evaluating the system calls based on the

set of usage rights as provided by O'Brien. Here the combination satisfies the need for a system

to control and monitor the access and use of restricted content on a network. See Rabne, column

3, lines 32-38. Additionally, O'Brien's kernel level enforcement provide more protection than

traditional security routines [see O'Brien, column 3 «lines 61-64»].

7.   Also concerning claims 1 and 9, the combination of Rabne and O'Brien did not explicitly

state obtaining the content on an individual block basis. Rabne, who teaches the distribution of

intellectual property over a network, is not specific on how this content is transferred; for

example Rabne is not specific as to whether it is transferred on an individual block basis.

However, obtaining content comprising data blocks from content sources on an individual block

basis is well known in the art as evidenced by Taylor whose system receives and filters each data

packet (which are transmitted individually) as well as a set of access policies that comprise a set

of predefined usage policies associated with the content for said user. Taylor's packets

correspond to Applicant's claimed "block." See also the response to Applicant's arguments

above. It would have been obvious to one of ordinary skill in the art at the time of the

applicant's invention to modify the combination of Rabne and O'Brien by adding the ability to

obtain content on an individual block basis as well as the access policies that comprise

predefined usage policies associated with the content for the user as provided by Taylor. Here

the combination satisfies the need for a system to control and monitor the access and use of

restricted content on a network. See Rabne, column 3, lines 32-38. The combination also

improves Rabne's system as it provides users the capability of dynamically filtering individual

packets [Taylor, column 4 «lines 8-12»].

8.   Some claims will be discussed together. Those claims which are essentially the same

except that they set forth the claimed invention as a method are rejected under the same rationale

applied to the described claim.

9.   Thereby, the combination of Rabne, O'Brien, and Taylor discloses:

*   <Claims 1 and 9>

        A dynamic file access control and management system configured to access one

or more content sources including a set of content, said system comprising:

        A. a proxy system linked to said one or more content sources, said proxy system

comprising an access control module configured to selectively obtain content comprising

data blocks from said content sources on an individual block basis as a function of an

authorization of a user requesting said content and a set of access policies (Rabne,

column 7, lines 5-9 and column 8, lines 55-67, where Taylor teaches obtaining the data

on an individual block basis, column 1 «lines 63-65» | column 5 «lines 32-39») that

comprise a set of predefined usage policies associated with the content for said user

(Rabne, column 8, lines 11-14 and 34-37 – Rabne's license agreement reads on

Applicant's claimed usage policy);

        B. a rights management module configured to generate a set of usage rights

associated with said content as a function of a set of predefined usage policies associated

with said content for said user (Rabne, column 8, lines 11-37 – permissions rights

generated from the license agreement);

C. at least one client device having a client module configured to interface to a

client operating system kernel, said client module configured to enforce the set of usage

rights within the operating system kernel without application rewrites (Rabne, column 6,

lines 31-45 and O'Brien, column 3 «lines 39-55» : O'Brien's kernel-level security

modules apply security policies by granting or denying access to resources), wherein

enforcing the set of usage rights includes:

intercepting a system call between an application and the client OS

[O'Brien, column 5 «lines 28-36» | column 7 «lines 10-12»];

evaluating the system call based on the set of usage rights [O'Brien,

column 5 «lines 56-66» | column 7 «lines 27-40»]; and

blocking or modifying the system call based on said evaluation [O'Brien

column 5 «line 67» to column 6 «line 4» | column 7 «lines 41-48»];

D. one or more communication means, via which said content and said usage

rights are provided to said client device (Rabne, column 3, lines 52-59).

- <Claims 2 and 10>

The system according to claim 1, wherein said content and said usage rights are

provided to said client device via different communication means (Rabne, column 10,

lines 34-48).

- <Claims 3 and 11>

    The system according to claim 1, wherein said content includes static content (Rabne, column 6, lines 53-60).

- <Claims 4 and 12>

    The system according to claim 1, wherein said content includes dynamic content (Rabne, column 6, lines 53-60).

- <Claims 5 and 13>

    The system according to claim 1, wherein said communication means includes a secure transform configured to encrypt and encapsulate said content into a message as a function of a session ID and said client is configured to extract said content from said message (Rabne, column 7, lines 10-19).

- <Claims 6 and 14>

    The system according to claim 1, wherein said proxy system further includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said content (Rabne, column 18, lines 20-32 and 50-67).

- <Claims 7 and 15>

    The system as in claim 1, wherein said client device is a device from a group comprising: 1) a personal computer; 2) a workstation; 3) a personal digital assistant; 4) an e-mail device; 5) a cellular telephone; 6) a Web enabled appliance; and 7) a server (Rabne, column 6, lines 31-45).

- <Claims 8 and 16>

    The system of claim 1, wherein said proxy system and at least one of said content

sources are hosted on the same computing device (Rabne, figure 1b, item 22).

    Since the combination of Rabne, O'Brien, and Taylor discloses all of the above

limitations, claims 1-16 are rejected.

10.   Claims 17 and 19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rabne,

O'Brien, and Taylor as applied to claims 1-16 above, in further view of Holden et al, U.S. Patent

No. 5.802.178 ["Holden"].

11.   With respect to claims 17 and 19, Rabne as modified by O'Brien and Taylor does not

expressly disclose the access control module of the proxy system further configured to encrypt

each data block of the content independently, using a unique initialization vector for each data

block and one or more encryption/decryption keys and wherein the one or more communication

means also provide the one or more encryption decryption keys to said client device. However,

these features were well known in the art at the time of Applicant's invention as evidenced by

Holden. Like Rabne, Holden is directed to a system providing security system policies that

regulate access control [column 5 «lines 33-52»]. Within this system, Holden discloses

encrypting each data block of the content independently, using a unique initialization vector for

each data block and one or more encryption/decryption keys [column 16 «line 64» to column 17

«line 10»], and providing the one or more encryption/decryption keys to a client [column 10

«lines 17-28» | column 19 «lines 9-12»: sharing an association key with other computers to be

used in decrypting the encrypted data block]. Holden's SNIU reads on the claimed access

control module. It would have been obvious to one of ordinary skill in the art to have modified

Rabne with the encryption functionality taught in Holden. One would have been motivated to

have so modified Rabne because Holden's encryption features provide greater security benefits

to Rabne's system [see Holden, column 3 «lines 18-25»].

12.   Thereby, the combination of Rabne, O'Brien, Taylor, and Holden discloses:

- «Claims 17 and 19»

The system according to claim 1:

wherein the access control module is further configured to encrypt each data block of the

content independently, using a unique initialization vector for each data block and one or

more encryption/decryption keys [*Holden*, column 16 «line 64» to column 17 «line 10»]; and

wherein the one or more communication means also provide the one or more encryption

decryption keys to said client device [*Holden*, column 10 «lines 17-28» | column 19 «lines 9-

12»: sharing an association key with other computers to be used in decrypting the encrypted

data block].

13.   Claim 18 is rejected under 35 U.S.C. §103(a) as being unpatentable over Rabne, O'Brien,

and Taylor as applied to claims 1-16 above, in further view of Shaath et al, U.S. Patent No.

7.392.234 ["Shaath"].

14.   As to claim 18, Rabne as modified by O'Brien and Taylor does not disclose each content

source stores a plurality of directories, at least one director including a plurality of content files

and a metafile, wherein the metafile stores a plurality of records, each record corresponding to

one of the plurality of content files within that directory, each record storing the set of predefined

usage policies associated with the corresponding content file as evidenced by Shaath. Like

Rabne, Shaath is directed towards a system for enforcing usage rights on content files [column 5

«line 67» to column 6 «line 11»]. Shaath discloses content source stores a plurality of directories

[column 5 «lines 44-54»], at least one director including a plurality of content files and a

metafile [column 5 «lines 55-61»: Shaath's policy reads on the claimed metafile | column 12

«lines 13-21»], wherein the metafile stores a plurality of records, each record corresponding to

one of the plurality of content files within that directory, each record storing the set of predefined

usage policies associated with the corresponding content file [column 11 «lines 23-30» | column

12 «line 13» to column 13 «line 28»]. It would have been obvious to one of ordinary skill in the

art to have modified Rabne's system to include Shaath's directory-based policy enforcement.

Rabne's system would be improved by implementing Shaath's teaching because it allows for a

hierarchical and automated application of file lifecycle policies [column 5 «lines 44-48» | column

6 «lines 12-17»].

15.   Thereby, the combination of Rabne, O'Brien, Taylor, and Shaath discloses:

- «Claim 18»

    The system according to claim 1, wherein each content source stores a plurality of

directories [column 5 «lines 44-54»], at least one director including a plurality of content files

and a metafile [column 5 «lines 55-61»: Shaath's policy reads on the claimed metafile | column

12 «lines 13-21»], wherein the metafile stores a plurality of records, each record corresponding

to one of the plurality of content files within that directory, each record storing the set of

predefined usage policies associated with the corresponding content file [column 11 «lines 23-

30» | column 12 «line 13» to column 13 «line 28»].

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to DOHM CHANKONG whose telephone number is (571)272-

3942. The examiner can normally be reached on Monday-Friday [8:30 AM to 4:30 PM].

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, John Follansbee can be reached on 571.272.3964. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dohm Chankong/
Examiner, Art Unit 2452